# VERITAS NetBackup 4.5 NetWare Media Server Option

## System Administrator's Guide

VERITAS

# Table of Contents

# Preface

This comprehensive manual provides detailed information and procedures for installing, configuring, and using the VERITAS NetBackup NetWare Media Server Option. Topics covered in this manual require the reader to have a working knowledge of the VERITAS NetBackup and the NetWare operating system. This manual is intended for the system administrator and other users.

## Organization

◆ Chapter 1 provides an overview of the NetBackup NetWare Media Server Option and its features.

◆ Chapter 2 provides intallation procedures for the NetBackup NetWare Media Server Option and the Open Transaction Manager and Intelligent Disaster Recovery options that come with it. This section also describes the installation requirements.

◆ Chapter 3 provides the steps for granting NetBackup access to the NetWare media server, and for setting up NetBackup to use the NetWare Media Server Option.

◆ Chapter 4 explains how to create manual backups of and restore data to the NetWare server using NetBackup and the NetWare Media Server Option and how to use the Open Transaction Manager (OTM) included with the NetWare Media Server Option.

◆ Chapter 5 describes how to use the Intelligent Disaster Recovery (IDR) Option, an option designed to help you quickly and efficiently recover your Novell NetWare servers after a catastrophic disaster.

## Related Documents

◆ *NetBackup for NDMP System Administrator's Guide*

This guide explains how to install, configure, and use VERITAS NetBackup for NDMP (Network Data Management Protocol).

See the following manuals if you are using and administrating NetBackup for NDMP on a UNIX host:

◆ *NetBackup Release Notes*

Provides other important information such as the platforms and operating systems that are supported and operating notes that are not in the manuals.

◆ *Media Manager Device Configuration Guide*

Provides information about configuring storage devices on UNIX systems.

◆ *NetBackup System Administrator's Guide - UNIX*

Explains how to configure and manage NetBackup.

◆ *NetBackup User's Guide - UNIX*

Explains how to perform backups, restores, and archives.

◆ *Media Manager System Administrator's Guide - UNIX*

Explains how to configure and manage the storage devices and media that NetBackup servers use for backups.

◆ *NetBackup Troubleshooting Guide - UNIX*

Provides troubleshooting information for the NetBackup product.

See the following manuals if you are using and administrating NetBackup for NDMP on a Windows NT/2000 host:

◆ *NetBackup Release Notes*

Provides important information about platforms and operating systems that are supported and operating notes that are not in the manuals.

◆ *NetBackup System Administrator's Guide - Windows NT/2000*

Explains how to configure and manage NetBackup.

◆ *NetBackup User's Guide - Windows NT/2000*

Explains how to perform backups, restores, and archives.

◆ *Media Manager System Administrator's Guide - Windows NT/2000*

Explains how to configure and manage the storage devices and media that NetBackup servers use for backups.

◆ *NetBackup Troubleshooting Guide - Windows NT/2000*

Provides troubleshooting information for the NetBackup product.

For more information about NDMP, see the following web site:

```
http://www.ndmp.org
```

# Online Documentation

## On Windows NT/2000

The released software contains on-line PDF and ASCII versions of these release notes and a readme file for the client. If you choose to install the documention during setup, NetBackup installs these documents in the following locations on your disk:

◆ *install_path*\Help\

Adobe Acrobat Portable Document Format (PDF) copies of all related documents, including these release notes.

◆ The readme files on *install_path*\NetBackup\ are:

- Readme.txt (The Readme.txt file (ASCII format) may be slightly more up-to-date than the printed and pdf copies of the release notes.)

- Readme_Client.txt

- Readme_Server.txt

- Readme_SMS.txt

- Readme_Win2000.txt

## On UNIX

During NetBackup installation, a text copy of the *NetBackup Media Manager Device Configuration Guide* is installed in

/usr/openv/volmgr/MediaMgr_DeviceConfig_Guide.txt

You can copy example code from the device configuration guide if you need to reconfigure the kernel to provide specific tape or optical peripheral support.

The product CD-ROM also contains PDF copies of these release notes and other documents.

**Note**  You will need Adobe Acrobat Reader to view the PDF documents. The latest version of Acrobat Reader is available on the Adobe web site: http://www.adobe.com.
VERITAS assumes no responsibility for the correct installation or use of the reader.

## On the Support Web Site

Copies of NetBackup documentation are also available on the VERITAS support web site:

1.  Go to the VERITAS support web page

    `www.support.veritas.com/`

2.  In the VERITAS Support Product List, choose NetBackup Products.

3.  A page appears with a list of the NetBackup products. Choose NetBackup
    BusinesServer or NetBackup DataCenter.

4.  The documents page appears. Choose the document you want.

# Conventions

The following conventions are used in this manual:

| | |
|---|---|
| **Steps** | Numbered steps are listed as 1., 2., …etc. |
| **Text that you type** | Text that you are required to type on the keyboard is shown in a lowercase font similar to what you would see on your screen. The text to be typed is preceded by the word *Type* and followed by the key(s) to press. |
| | For example, Type: `a:install` and press <Enter>. |
| **Selections that you make** | Selections you need to make from the user interface appear in both upper and lowercase in a sans serif font. |
| | For example, From the Options menu, click Preferences. |
| **Path and path variables** | When a path name is presented, a serif font that is slightly larger than normal type is used. Path variables appear in italics. |
| | For example, *server name*\\*sys volume*\VERITAS\NBU |
| **Keys** | Keys appear in angle brackets (< >). |
| | For example, <Enter>, <Esc>, <Del>, etc. |
| | When two or more keys need to be pressed simultaneously to perform a function, they appear in angle brackets with a plus sign. For example, <Shift + F1>. |
| **Hot keys or accelerator keys** | If there is a shortcut key, it is shown in the application next to the menu choice. If there is a toolbar button or another shortcut, it will be noted in the documentation as a tip. |

# Terms

The terms listed in the table below are used in the VERITAS NetBackup documentation to increase readability while maintaining technical accuracy.

| Term | Definition |
|------|------------|
| Microsoft Windows, Windows | Terms used as nouns to describe a line of operating systems developed by Microsoft, Inc. |
| | A term used as an adjective to describe a specific product or noun. Some examples are: Windows 95, Windows 98, Windows NT, Windows 2000, Windows servers, Windows clients, Windows platforms, Windows hosts, and Windows GUI. |
| | Where a specific Windows product is identified, then only that particular product is valid with regards to the instance in which it is being used. |
| | For more information on the Windows operating systems that NetBackup supports, refer to the VERITAS support web site at `http://www.support.veritas.com`. |
| Windows servers | A term that defines the Windows server platforms that NetBackup supports; those platforms are: Windows NT and Windows 2000. |
| Windows clients | A term that defines the Windows client platforms that NetBackup supports; those platforms are: Windows 95, 98, ME, NT, 2000, XP (for 32- and 64-bit versions), and LE. |

# Getting Help

For updated information about this product, including system requirements, supported platforms, supported peripherals, and a list of current patches available from Technical Support, visit our web site:

```
http://www.support.veritas.com/
```

VERITAS Customer Support has an extensive technical support structure that enables you to contact technical support teams that are trained to answer questions to specific products. You can contact Customer Support by sending an e-mail to support@veritas.com, or by finding a product-specific phone number from the VERITAS support web site. The following steps describe how to locate the proper phone number.

1. Open `http://www.support.veritas.com/` in your web browser.

2. Click **Contact Support**. The *Contacting Support Product List* page appears.

3. Select a product line and then a product from the lists that appear. The page will refresh with a list of technical support phone numbers that are specific to the product you just selected.

# Introducing NetBackup NetWare Media Server Option 1

This section provides an overview of the NetBackup NetWare Media Server Option and its features.

*Introducing NetBackup NetWare Media Server Option* includes the following topics:

| Section | Describes |
|---------|-----------|
| "About NetBackup NetWare Media Server Option" on page 1 | An overview of the NetWare Media Server Option, how it works in conjunction with NetBackup and NetBackup for NDMP, and introduces some of the terminology used with this application. |
| "NetBackup NetWare Media Server Option Features" on page 3 | The features that are offered by the NetWare Media Server Option. |

## About NetBackup NetWare Media Server Option

NetBackup NetWare Media Server Option is a separately purchased option for VERITAS NetBackup 4.5 that provides a NetWare media server for NetBackup. With the NetWare Media Server Option, you can control backups and restores of the NetWare media server from a central NetBackup server, but the storage devices used for these backups and restores are attached locally to the NetWare server.

The NetBackup master or media server uses the Network Data Management Protocol (NDMP) to control the backups and restores on the NetWare server, which serves as an *NDMP host*. The host is considered a client of NetBackup, but NetBackup client software is not installed on an NDMP host.

Instead, the NetWare Media Server Option performs backups and restores of the NetWare server as directed by commands that it receives from NetBackup.

NDMP Architecture Using NetWare Media Server Option



Network Connection

NetBackup with
NetBackup for NDMP

NetWare Media Server
(NDMP Host)
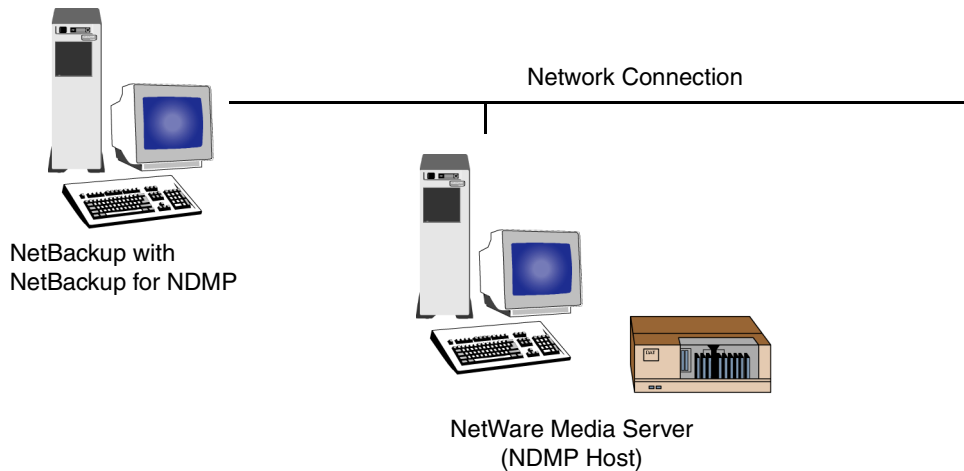
The backup or restore can be a *local* backup or restore, in which the data travels from the NetWare media server to its locally attached storage devices, such as tape drives or robotic libraries. Or, the data can travel over the network between the NetWare media server and a storage device attached to another NDMP host in what is known as a *three-way* backup or restore.

Local Versus Three-Way Backups and Restore

NetBackup with
NetBackup for NDMP



**Three-Way Backup/Restore Using Network Connection**

**Local Backup/Restore**

NetWare Media Server
(NDMP Host)

Another NDMP Host
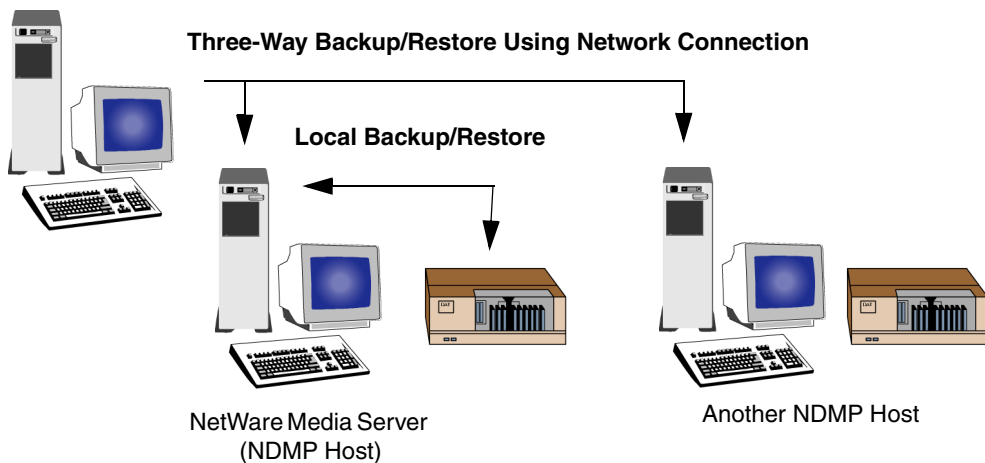
The NetWare Media Server Option includes the Open Transaction Manager (OTM) and Intelligent Disaster Recovery (IDR) options. With the Open Transaction Manager, you can back up files that are in use without having to first lock those files. The Intelligent Disaster Recovery option is a fully-automated disaster recovery solution that allows you to quickly and efficiently recover your computers after a disaster.

# NetBackup NetWare Media Server Option Features

NetBackup NetWare Media Server Option includes the following features:

◆ *High speed local backup of a NetWare Media Server*. Backup data travels between disk and tape drives attached directly to the same NetWare Media Server, providing high-speed backup without increasing network traffic.

◆ *Centralized backup policy management*. You can manage backup tasks, such as scheduling jobs and managing catalogs from a NetBackup master server.

◆ *Device and media management*. NetBackup Media Manager provides total management and control of the devices and media used for backups and restores of NetWare Media Servers.

◆ *Shared robots*. You can share robots between NetWare Media Servers and NetBackup servers or between multiple NetWare Media Servers. Robotic control can be on an NetWare Media Server or on a NetBackup server. If the robot is a tape library DLT (TLD) or tape library 8MM (TL8) robot, some of the tape drives can attach to NetWare Media Servers and other drives can attach to NetBackup servers.

◆ *Cluster support.* The NetWare Media Server Option supports clustering. To ensure that all volumes are protected, you must run the NetWare Media Server Option on all NetWare servers in the cluster and create backup jobs that protect clustered volumes on all servers in the event of a failover. For more information about running the NetWare Media Server Option in a cluster, see "Using the NetWare Media Server Option With a Cluster" on page 36.

# Installing NetBackup NetWare Media Server Option    2

This section explains how to install NetBackup NetWare Media Server Option and the Open Transaction Manager and Intelligent Disaster Recovery options that come with it. This section also describes the installation requirements.

*Installing NetBackup NetWare Media Server Option* includes the following topics:

| Section | Describes |
|---|---|
| "Installation Requirements" on page 5. | Provides the minimum requirement for installing this option and steps for verifying the amount of memory on the media server. |
| "Installing NetBackup NetWare Media Server Option" on page 6. | Provides steps for installing this option. |

## Installation Requirements

Before you install NetBackup NetWare Media Server Option, be sure that your media server meets the following minimum requirements:

◆ Novell NetWare 4.2x or later

◆ 8 MB RAM over server requirements

◆ 30 MB disk space

◆ Compatible tape device and controller

◆ TCP/IP

## Verifying the Amount of Memory on the Media Server

NetBackup requires a minimum of 8 MB of memory above the standard NetWare memory requirements. The amount of memory required increases as you add more tape devices. If you do not have the minimum amount of memory required when you install NetBackup NetWare Media Server, your system performance will suffer.

▼ **To verify that the Media Server has sufficient memory to install NetBackup NetWare Media Server Option:**

1. At the server console, type **load MONITOR.NLM**.

2. Press <Enter>.

3. Select **System Resources**.

**Note**  If you are using a version of NetWare prior to 5.x, select **Resource Utilization**.

The Server Memory Statistics dialog box displays. If the number next to **Cache buffers memory** is less than 65%, the memory is too low. To increase this number, unload some NLMs that may be using a large amount of memory or add more memory to the server before you install NetBackup NetWare Media Server Option.

# Installing NetBackup NetWare Media Server Option

Install NetBackup NetWare Media Server Option from a Windows workstation to each server you want to protect.

▼ **To install NetBackup NetWare Media Server Option:**

1. Insert the installation CD into the Windows workstation's CD-ROM drive.

2. From the installation CD browser, select **NetBackup Installation**.

3. Select **Start NetBackup Server Installation**.

4. Click **OK**.

   The Welcome window appears.

5. Click **Next** to proceed with the installation.

   The License Agreement window appears.

6. Read the license agreement, and then select **I accept the terms of the license agreement**.

7. Click **Next**.

8. Select the options you want to install. Your choices are:

   - **NetBackup NetWare Media Server Option**. Select this option to install the NetBackup NetWare Media Server Option to the server you select.

   - **Open Transaction Manager**. Select this option to back up files that are in use without having to lock the files during the backup.

   - **Intelligent Disaster Recovery**. Select this option to install the Intelligent Disaster Recovery option, which allows you to restore a NetWare server in its entirety.

9. Click **Next**.

10. If the NetWare server on which you want to install the files appears in the **Available Servers** list, select the server, and then click the right arrow to move it to the **Destination Systems** list.

    If the NetWare server does not appear in the list, click **Manually add additional systems**, and then type the name of the server.

**Note**  Only one server at a time can be selected as the Destination System.

11. Click **Next**.

**Note**  The server icon in **Destination Systems** displays green if you are connected. If you are not connected, the icon displays red.

12. If you are already connected to the server, click **Next**.

    If you are not connected to the server:

    a. Click the server's icon in **Destination Systems**.

    b. Type the user name and password.

    c. Click **Connect**.

    d. Click **Next**.

13. If you are satisfied with the settings that display, click **Next**.

If you are not satisfied with the settings, click **Back** until you reach the information you want to change.

The files are copied to *server name\sys volume*\VERITAS\NBU.

**14.** If you want the NetBackup NetWare Media Server to load automatically when the server starts, click **Yes**; otherwise, click **No**.

**15.** Click **Finish** to view the ReadMe file and complete the installation.

## Setting Up the Account Name and Password

When NetBackup is first started, a default user name and password is created. If you do not want to use this account, you can create your own account name and password. You only have to set up the account and password once.

**Note** When setting up the NDMP account name, you must provide a *fully distinguished* name, such as .admin.novell. A fully distinguished, or complete, name consists of different object types, such as common name (CN), Organizational Unit (OU) objects, and Organization (O) objects.

▼ **To set up the account name and password on the server:**

**1.** On the server console type **load NDMPD -a** followed by the account name and the name of the context where the account name resides in the directory tree and **-p** followed by the password.

Example: ndmpd -a.admin.veritas -padmin

**Note** If you type **load NDMPD**, you will be prompted to enter user credentials.

**2.** Press <Enter>.

The setup is complete. You can now start the NetBackup NetWare Media Server Option.

## Starting NetBackup NetWare Media Server Option

▼ **To start NetBackup:**

   **1.** From your system console prompt, type:

   **nbustart**

   **Note**  The first time you type **nbustart** you will be prompted for user credentials.

   **2.** Press <Enter>.

# Configuring NetBackup for the NetWare Media Server Option

<div style="text-align:right">**3**</div>

This section provides the steps for obtaining information from the NetWare server that will be used when configuring drives, robots, storage units, and policies used for protecting the NetWare media server. This section also describes the steps for granting NetBackup access to the NetWare media server, and for setting up NetBackup to use the NetWare Media Server Option.

*Configuring the NetBackup NetWare Media Server Option* includes the following topics:

| Section | Describes |
|---------|-----------|
| "Obtaining Device, File System, and Host Information" on page 11 | How to display and print device, file system, and host information that must used in NetBackup when setting up policies and storage units for the NetWare media server. |
| "Providing Access to the NDMP Host" on page 12 | The procedures for authorizing the NetBackup media server with access to the NetWare media server. |
| "Adding Devices, Storage Units, and Policies" on page 16 | How to set up NDMP storage devices, storage units, and policies for NetBackup to use for automatic backups of the NetWare server data. |

## Obtaining Device, File System, and Host Information

Device, file system, and host information for your NetWare media server is needed when setting up storage units and policies in NetBackup for protecting the NetWare data.

▼ **To obtain device, file system, and host information:**

1. On the NetWare server's System Console, type:

   ```
   ndmpcfg
   ```

2. Press <Enter>.

The information displays on the screen and is also placed in a file called `ndmpconfig` in the root directory of the volume (`SYS:\`).

**3.** Navigate to `SYS:\` and print the `ndmpcfg.log` file.

Keep the print out on hand while you set up access to the NDMP host, and set up devices, storage units, and policies.

# Providing Access to the NDMP Host

For the NetBackup media server to control backups and restores on the NetWare media server, you must first provide the NetBackup for NDMP server access to the NetWare NDMP host. To provide this access, you must add the NDMP host information to the NetBackup for NDMP server's Hosts file , and then authorize access to the NDMP host. If robotic libraries are attached to the NetWare media server, you must configure robotic control by specifying the device name, controller number, SCSI ID, and LUN (logical unit number) on the NetBackup for NDMP server before verifying access to the NDMP host.

## Adding the NDMP Host Information to the Hosts File

If you are not using Domain Name Services (DNS), then the IP addresses for the NetWare servers you want to communicate with must be included in the NetBackup for NDMP server's Hosts file.

▼ **To add your NetWare server's address to the NetBackup Server's Hosts file:**

**1.** Open the Hosts with a text editor, such as Notepad.

**2.** On a blank line, type the IP address of the NetWare server, followed by at least one space, and then the server's name.

**3.** Save the Hosts file.

**Note** The Hosts file should *not* have a file name extension.

## Authorizing Access to the NDMP Host

Before you can use NetBackup for backup or restore operations on the NetWare media server, you have to provide NetBackup with access to the NDMP host. If you plan to run three-way backups, you must provide access to both the NDMP host that does not have a storage device attached to it as well as the NDMP host with the storage devices attached.

**Note** If you have not entered the IP address for your NDMP host in the Hosts file of your workstation, you must enter the IP address rather than the NDMP host name.

▼ **To authorize access to the NDMP host:**

1. On a DOS command line on the NetBackup for NDMP server on a Windows system, type:

   *install_path*\Volmgr\bin\set_ndmp_attr -auth *ndmp_host user_name*

   For a UNIX system, type:

   *install_path*/Volmgr/bin/set_ndmp_attr -auth *ndmp_host user_name*

   **Note** The default install path for a Windows system is C:\Program Files\Veritas; for a UNIX system, the default install path is /usr/openv/.

   *NDMP_host* is the name of the NDMP host that NetBackup will be backing up. *User_name* is the user name under which NetBackup will access the NDMP host. This user must have persmission to execute the NDMP commands.

   In the following example, *C:\Program Files* is the install path, *darva* is the NDMP_host, and *admin* is the user_name.

   C:\Program Files\Volmgr\bin\set_nmdp_attr -auth darva admin

   You will be prompted to enter the password twice. The default NetWare Media Server Option password is **bex**.

2. Enter **bex**.

3. Press <Enter>.

4. Enter **bex**.

   Entering **bex** authorizes the use of the NetWare Media Server Option by NetBackup.

5. Press <Enter>.

# Configuring Robotic Control

If your NetWare media server has robotic libraries attached, you must configure robotic control using the `set_ndmp_attr -robot` command.

▼ **To configure robotic control:**

❖ On a DOS command line on the NetBackup for NDMP server on a Windows system, type:

    install_path\Volmgr\bin\set_ndmp_attr -robot NDMP_host
    robot_device scsi_controller scis_id scsi_lun

For a UNIX system, type:

    install_path/Volmgr/bin/set_ndmp_attr -robot NDMP_host
    robot_device scsi_controller scis_id scsi_lun

**Note** The default install path for a Windows system is C:\Program Files\Veritas; for a UNIX system, the default install path is /usr/openv/.

*NDMP_host* is the name of the NetWare media server serving as the NDMP host to which the robotic library is attached.

*Robot_device* is the device name for the robot.

*SCSI_controller* is the controller number.

*SCSI_ID* is the SCSI ID for the robot.

*SCSI_lun* is the LUN for the robot.

After all configurations have been entered for all robots attached to your NetWare media server, you can list your configuration settings by again typing the set_ndmp_attr command followed by the -list option. For example, if your NetBackup media server is a Windows system, you would type:

    install_path\Volmgr\bin\set_ndmp_attr -list

**Note** If you change the robot configuration on the NDMP host, use `set_ndmp_attr -robot` to update the NetBackup for NDMP server with your changes.

## Verifying Authorization

After you have entered the authorization and configured robotic control for all libraries attached to your NetWare media server, verify that the NetBackup for NDMP server can connect to the NDMP host.

▼ **To verify connection to the NDMP host:**

❖ On a DOS command line on the NetBackup for NDMP server on a Windows system, type:

`install_path\Volmgr\bin\set_ndmp_attr -verify NDMP_host`

For a UNIX system, type:

`install_path/Volmgr/bin/set_ndmp_attr -verify NDMP_host`

**Note** The default install path for a Windows system is C:\Program Files\Veritas; for a UNIX system, the default install path is /usr/openv/.

Verifying Host Connection

```
C:\Program Files\VERITAS\Volmgr\bin>set_ndmp_attr -verify darva
Connecting to host "darva" as user "admin"...
Waiting for connect notification message...
Opening session--attempting with NDMP protocol version 3...
Opening session--successful with NDMP protocol version 3
  host supports MD5 authentication
Getting MD5 challenge from host...
Logging in using MD5 method...
Host info is:
  host name "DARVA"
  os type "NetWare"
  os version "v5.0"
  host id "6932430a"
Login was successful
Host supports LOCAL backup/restore
Host supports 3-way backup/restore
Opening SCSI device "/dev/scsi/_00_05_00"...
Setting SCSI target controller 0 id 5 lun 0...
Inquiry result is "ADIC    FastStor DLT    D18A"

C:\Program Files\VERITAS\Volmgr\bin>
```

# Adding Devices, Storage Units, and Policies

For NetBackup to use the NetWare Media Server Option to launch backups on the NetWare media server, you must first create for each NDMP host:

◆ Storage devices (see "Adding NDMP Storage Devices" on page 16)

◆ Storage units (see "Creating NDMP Storage Units" on page 21)

◆ Policies (see "Creating NDMP Policies" on page 23)

These are created from the NetBackup master or media server using the information you obtain from your NetWare media server (see "Obtaining Device, File System, and Host Information" on page 11).

## Adding NDMP Storage Devices

You must use Media Manager to add the drives and robots that attach to the NDMP host before NetBackup can use them as storage devices and before you can create a storage unit for these devices (see "Creating NDMP Storage Units" on page 21).

**Note** You cannot use the NetBackup wizards to configure robots or drives that are attached to the NDMP host.

▼ **To add a robot attached to an NDMP host:**

**1.** If the NetBackup for NDMP server is a Windows NT/2000 system, click **Start**, point to **Programs**, point to **VERITAS NetBackup**, and click **NetBackup Administration**.

If the NetBackup for NDMP server is UNIX system, type:

/usr/openv/netbackup/bin/jnbSA &

**2.** From the right pane of the NetBackup Administration window, click **Devices**.

**Note** If you are not running NetBackup Administration on the NetBackup for NDMP server, use the **Monitor** command on the **Hosts** menu to switch to the NetBackup for NDMP server.

**3.** Click **Actions** menu, select **New**, and then select **Robot**.

**4.** Complete the options for the Add Robot dialog box. The options are described in "Add Robot Dialog Box" on page 17.

**5.** Click **OK**.

**6.** If you have additional robots or drives to add, click **No** when prompted if you want to stop and restart the NetBackup Device Manager service. When all robots and drives have been added, click **Yes** on this prompt.

▼ **To add a drive attached to the NDMP host:**

**1.** If the NetBackup for NDMP server is a Windows NT/2000 system, click **Start**, point to **Programs**, point to **VERITAS NetBackup**, and click **NetBackup Administration**.

If the NetBackup for NDMP server is UNIX system, type:

/usr/openv/netbackup/bin/jnbSA &

**2.** From the right pane of the NetBackup Administration window, click **Devices**.

**Note** If you are not running NetBackup Administration on the NetBackup for NDMP server, use the **Monitor** command on the **Hosts** menu to switch to the NetBackup for NDMP server.

**3.** From the **Actions** menu, select **New**, and then select **Drive**.

**4.** Complete the options for the Add Drive dialog box. The options are described in "Add Drive Dialog Box" on page 20.

**5.** Click **OK**.

## Add Robot Dialog Box

The Add Robot dialog box allows you to enter information about robots attached to your NetWare server.

Add Robot Dialog Box



Options on this dialog include:

◆ **Device host**. Specify the Media Manager host to which you are adding the robot. The host shown by default is the device host you selected earlier in the tree. If you want to specify a different host, select a name from the list, or use the browse button to select a host not appearing in the list.

◆ **Robot type**. Select the type of robot you are adding.

◆ **Robot number**. Specify a unique, logical identification number for the robot. This number identifies the robot in listings, such as Robot 1 - TLD. You also use this number when adding the robot's media to the Media Manager configuration. Robot numbers must be unique for all physically-distinct robots on all hosts in the configuration, regardless of the robot type or the host that controls them. For example, there cannot be two robots with robot number 1, even if the robots are

controlled by and configured on different hosts. If you are adding a robot definition for a robot controled by a remote device host, be sure to use the same robot number for that robot on all other device hosts.

◆ **Volume database host**. Specify the name of the host where Media Manager keeps the volume configuration information about the media in the robot. You must know the name of the volume database host when adding volumes to the robot. You can specify any Media Manager host as the volume database host, even if the host does not have any attached drives or robots.

---

**Caution** It is recommended that you use one volume database host for all your volumes (robotic and stand-alone drives). Although it is possible to maintain separate volume databases on multiple hosts, administration is more difficult and it is not possible to merge databases.

---

◆ **Robot control**. Select the option **Robot control is attached to an NDMP host**.

◆ **Robot device**. Click **Browse**, and then specify the controller number, SCSI ID, and SCSI LUN information for the robot device that is attached to the NDMP host. This information can be obtained on the SCSI section of the NDMPCFG printout (see "Obtaining Device, File System, and Host Information" on page 11).

◆ **NDMP host name**. Enter the name of the NetWare media server.

## Add Drive Dialog Box

The Add Drive dialog box allows you to enter information about the drives attached to your NetWare server.

Add Drive Dialog Box



Options on this dialog box include:

◆ **Device host**. Specify the Media Manager host to which you are adding the drive. The host shown by default is the device host you selected earlier in the tree. If you want to specify a different host, select a name from the list, or use the browse button to select a host not appearing in the list.

◆ **Drive type**. Specify the type of drive you are adding.

◆ **Drive name**. Enter the name that will be used by the Media Manager to identify the drive. Descriptive names are recommended.

◆ **Device name**. Name of the physical device on the NetWare system preceded by the host name and a colon. This information can be obtained on the Tape section of the NDMPCFG printout (see "Obtaining Device, File System, and Host Information" on page 11).

◆ **Drives is in a robotic library**. Select this option if the drive is in a robotic library. Clear this option if the drive is a stand-alone drive.

◆ **Robotic library**. If **Drive is in a robotic library** is selected, select the robot that controls the drive. If the robotic library does not appear in the drop-down list, it has not yet been added.

◆ **Robot drive number**. Select the robot drive number assigned to this drive.

## Creating NDMP Storage Units

An NDMP storage unit consists of one or more storage devices of a specific type and density that are attached to an NDMP host but are controlled by NetBackup's Media Manager. NetBackup stores data on these storage units during a backup of the NDMP host. Before setting up storage units, add the robots and devices that will be used by the NDMP host through the Media Manager (see "Adding Devices, Storage Units, and Policies" on page 16).

Refer to the *NetBackup System Administrator's Guide* (Windows NT/2000 or UNIX) for the procedures for creating the storage units. Enter the following options on the **Add New Storage Unit | General Properties** tab:

◆ **Storage unit type**. Select NDMP from the drop-down list.

◆ **On demand only**. Select this option if the storage unit is to be available only when a policy or schedule requests it; otherwise, the storage unit is available to any NDMP policy or schedule. Select this option if both of the following conditions exist:

- The NDMP host with the storage unit is the only one in the policy.

- There is more than one storage unit for the NDMP host, and you want to use the storage units for specific schedules. For example, you can set up schedules to use one storage unit for full backups while another storage unit is set up use with incremental backups.

Storage Unit Type Properties Tab



On the **Add New Storage Unit | Storage Unit Type Properties** tab, complete the following options:

- ◆ **NetBackup media server (NDMP client)**. Defaults to the name of the local NetBackup for NDMP server that will control backups for the NDMP media host.

- ◆ **NDMP host**. Enter or use **Browse** to select the name of the NetWare media server.

- ◆ **Robot type**. Select the type of robot (if any) that the storage unit contains, or if the device is a stand-alone drive, select **NONE - Not Robotic**.

- ◆ **Robot number**. For a robotic storage unit, this is the same robot number used when adding the robot.

- ◆ **Density**. Specify the media density that the storage unit will use.

- ◆ **Maximum concurrent drives used for backup**. Specify the number of drives that NetBackup can use at one time for backups using this storage unit. The number cannot be more than the total number of drives assigned to this storage unit.

## Creating NDMP Policies

The backup policy that sets rules for backing up the NDMP host must be created on the NetBackup master server following the procedures outlined in the *NetBackup System Administrator's Guide* (Windows NT/2000 or UNIX).

Add New Policy - Attributes Tab



For the NetWare Media Server Option, specify the following policy attributes:

◆ **Policy type**. Select NDMP from the drop-down list of policy types. Policy type determines the type of clients that can be protected by this policy.

◆ **Policy storage unit**. Specify the name of the storage unit that will be used for this policy. For local backups, the Policy storage unit must be attached to the NDMP host. For three-way backups, you can specify a storage unit on another NDMP host.

Add New Policy - Clients Tab
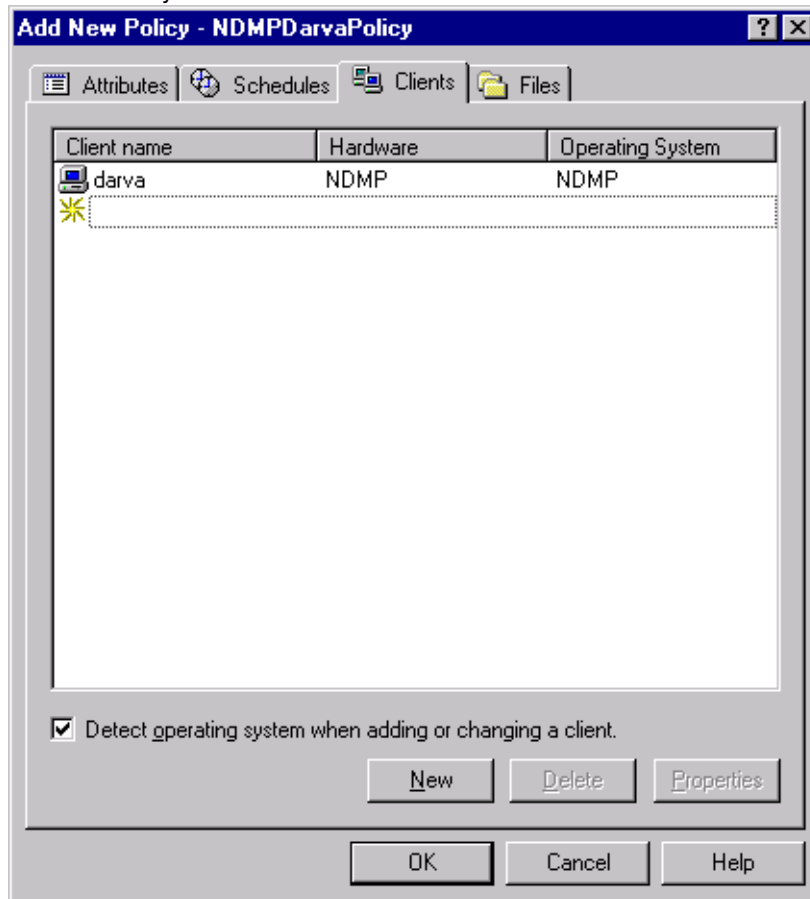


In the client list, specify the following for each client in an NDMP policy:

◆ **Client name**. Enter the name of the NetWare server.

◆ **Hardware and operating system**. Select NDMP NDMP.

When selecting the files to be automatically backed up, provide the directory name as part of the file. For example, \\*NDMP host*\sys\logs\. Wildcards cannot be used in pathnames for an NDMP policy, and you cannot provide an **Exclude list**, although you can use the **SET** option as an environmental variable to exclude files on a backup.

## Using Environmental Variables in a File List

On the **Add New Policy - Files** tab, you can use environmental variables to pass configuration parameters to the NetWare media server with each backup and restore. NDMP environmental variables can include variables that are:

◆ Defined as optional by the NDMP specification.

◆ Specific to an NDMP host vendor.

Add New Policy - Files Tab
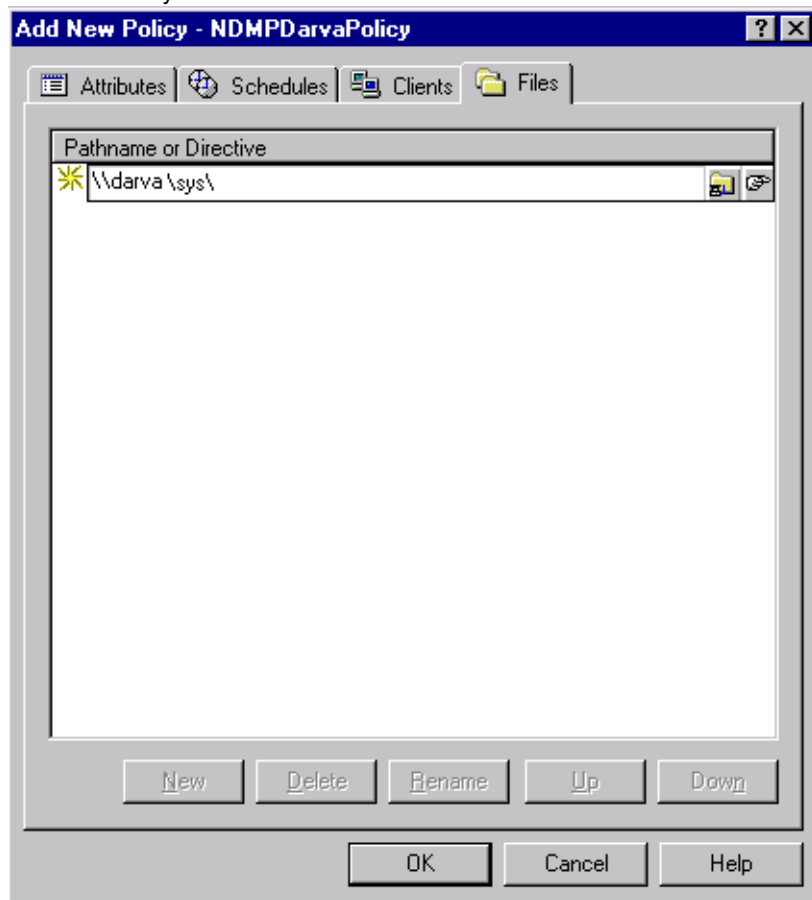


Variables reserved for use by NetBackup include:

◆ FILESYSTEM

◆ LEVEL

◆ DIRECT

- ◆ EXTRACT
- ◆ ACL_START

You can set variables defined as option by NDMP or specific to an NDMP host vendor by specifying one or more SET directives, using the following syntax:

```
SET variable = value
```

Variable is the name of the environment variable and value is the value assigned to the variable. The value can be enclosed in single or double quotes, and must be enclosed in quotes if it contains a space character.

Setting a variable equal to no value removes the variable. For example:

```
SET ABC =
```

**Note** The set command entry must occur in the file list before the directories and files to which it applies.

Variables accumulate as the file list is processed. For example, suppose the file list contains the following entries:

```
SET HIST = N

\\NDMP Host\SYS\

SET HIST = Y

\\NDMP Host\USER\
```

The entire SYS volume would be backed up without sending any file history. The USER volume would then be backed up and file history information would be sent.

If an environment variable appears again in the list, the second value listed overrides the previous value of the variable.

The values used in each backup are saved and provided to subsequent restores of the directory. The NDMP host may have environment variables that are set internally; these are also saved for restores.

The type of data that can be backed up on the server will be listed in the NDMPCFG file, along with the syntax required for entering this information. For example:

```
\\server name\Server Specific Info\
```

## Setting Schedules

The schedule for your NDMP backup is set in the **Add New Policy - Schedule** tab.

Add New Policy - Schedule Tab
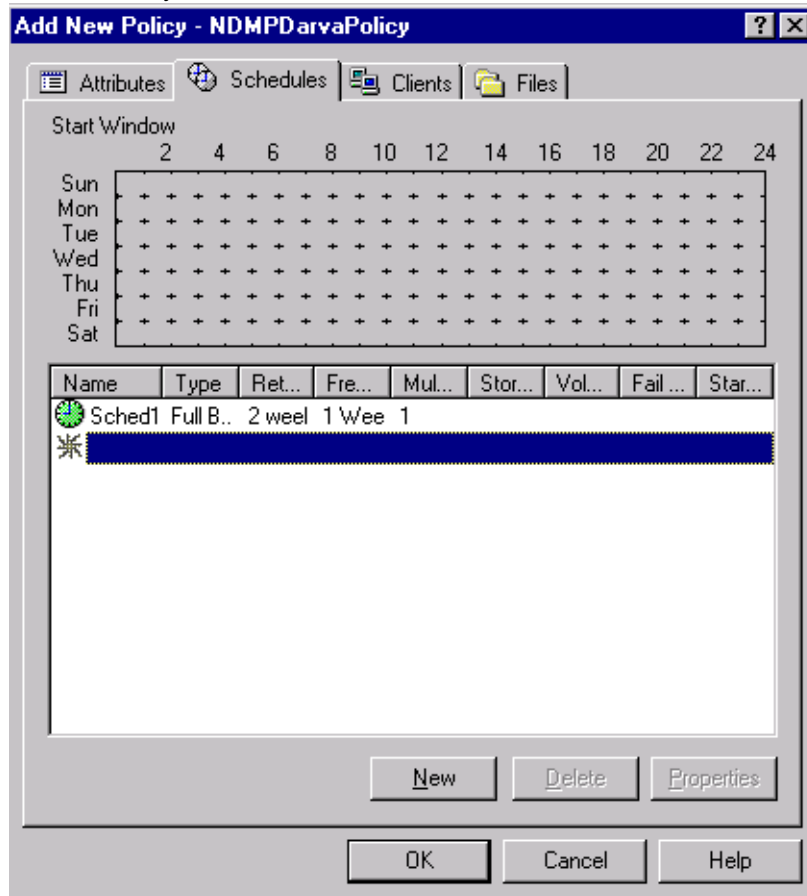


You can select any of the following backup types in a schedule for an NDMP policy:

◆ **Full**. Backs up all files in the file list for the policy, regardless of when they were last modified or backed up. If you use incremental backups, you must also schedule full backups to perform a complete restore.

◆ **Cumulative Incremental**. Backs up all files in the file list that have changed since the last successful full backup. All files are backed up if no prior backup was done. When this backup type is used, a complete restore of your system requires the last full and the last cumulative incremental backup.

♦ **Differential Incremental**. Backs up all files in the file list that changed since the last incremental or full backup. When this backup type is used, a complete restore of your system requires the last full backup and all differential backups made since the last full backup.

Specify **Override policy storage unit** only if the NetWare server has more than one storage unit and you want to use a specific storage unit for this schedule. The NetWare server must be the only client in the NDMP policy.

# Using the NetWare Media Server Option 4

This section explains how to create manual backups of and restore data to the NetWare server using NetBackup and the NetWare Media Server Option. This section also addresses how to use the Open Transaction Manager (OTM) included with the NetWare Media Server Option.

*Using the NetWare Media Server Option* includes the following topics:

| Section | Describes |
|---------|-----------|
| "Performing a Backup" on page 29 | How to create a backup job using the NetWare Media Server Option. |
| "Performing a Restore" on page 30 | How to restore data using the NetWare Media Server Option. |
| "Using the Open Transaction Manager" on page 32 | How to protect open files using the Open Transaction Manager and the NetWare Media Server Option. |

## Performing a Backup

User-directed backups of the NetWare system serving as the NDMP host are not permitted. Instead, backups can either be created automatically or manually by the administrator on a NetBackup server. Automatic, unattended backups are created by NetBackup based on the creation of policies and schedules (see "Creating NDMP Policies" on page 23 and "Setting Schedules" on page 27).

You cannot back up files where the path length is greater than 1024 characters. You can only include directory or volume paths and cannot use wildcards in the file list for an NDMP policy.

▼  **To create a manual backup of an NDMP policy:**

1.  If the NetBackup for NDMP server is a Windows NT/2000 system, click **Start**, point to **Programs**, point to **VERITAS NetBackup**, and click **NetBackup Administration**.

    If the NetBackup for NDMP server is UNIX system, type:

    ```
    /usr/openv/netbackup/bin/jnbSA &
    ```

2.  From the NetBackup Administration window, click the **Backup Policy Management** icon.

3.  Click the NDMP policy name in the left pane.

4.  From the **Policy** menu, select **Manual Backup**.

5.  On the Manual Backup dialog, select the schedule and the NDMP hosts that you want to backup up.

    If you do not select a schedule, NetBackup uses the schedule with the highest retention level. If you do not select an NDMP host, NetBackup backs up all NDMP hosts.

6.  Click **OK**.

# Performing a Restore

User-directed restores are not allowed. Instead, the administrator can restore files to the NDMP host from which they were backed up by creating a restore job from the NetBackup server. Files backed up from an NDMP storage unit cannot be restored from a non-NDMP storage unit.

**Caution**   An NDMP restore always overwrites existing files.

▼  **To perform a restore from a Windows NT/2000 NetBackup server:**

1.  Click **Start**, point to **Programs**, point to **VERITAS NetBackup**, and click **NetBackup Administration**.

2.  From the NetBackup Administration **File** menu, click **Backup, Archive, and Restore**.

3.  From the Backup, Archive, and Restore window, click **Select for Restore** from the tool bar.

**4.** From the **Actions** menu, click **Specify NetBackup Machines**.

The Specify NetBackup Machines dialog appears. Modifications made in this dialog affect all open restore windows and are not saved after closing the Restore window.

**5.** On the **Servers** tab, specify the NetBackup master server. If your configuration has multiple master servers, specify the master server that has the policy for the NDMP host you are restoring.

**6.** Click **Make Current**.

**7.** On the **Source Clients** tab, specify the NetWare server on which the storage unit is attached.

**8.** In the **Policy Type** field, select **NDMP**.

**9.** On the **Destinations Clients** tab, select the NetWare server you want to restore to, and then click **OK**.

**10.** On the Restore window, browse and mark the files and folders you want to restore.

**11.** From the **Action** menu, click **Start Restore of Marked Files**.

**12.** Complete the options on the Restore Marked Files dialog.

**13.** Click **Start Restore**.

▼ **To perform a restore from a UNIX NetBackup server:**

**1.** Type:

```
/usr/openv/netbackup/bin/jnbSA &
```

**2.** Click the **Backup, Archive, and Restore** icon on the right panel.

The Backup, Archive, and Restore window appears. Modifications made in this window affect all open restore windows and are not saved after closing the restore window.

**3.** From the **Action** menu, select **Specify NetBackup Machine**.

**4.** On the **NetBackup server** tab, specify the NetBackup master server. If your configuration has multiple master servers, specify the master server that has the policy for the NDMP host you are restoring.

5.  On the **Source client** tab, specify the NetWare server on which the storage unit is attached.

6.  In the **Policy Type** field, select **NDMP**.

7.  On the **Destination client** tab, select the NetWare server you want to restore to.

8.  Browse and mark the files and folders you want to restore.

9.  Click **Restore**.

10. Complete the options on the Restore Files dialog.

11. Click **Start Restore**.

# Using the Open Transaction Manager

The Open Transaction Manager (OTM) allows you to back up open files on your NetWare media server serving as the NDMP host. OTM must be installed on the NetWare system along with the NetWare Media Server Option.

After OTM is installed, it runs in the background of the NetWare server, waiting for a job using OTM to run. When a backup job using OTM starts, a point-in-time or static view of the volume is created. This static, unchanging view of the volume is then backed up and released when the backup completes.

During a backup using OTM, if changes are made to the original data, OTM makes a duplicate of the original data before it is changed and stores this duplicate in a buffer. This buffer, combined with the unchanged portions of the volume, gives you the static view of the volume when the backup started. By default, the buffered data is stored in a file named SYS:\SYSTEM\OTM01; however, you can designate another file, directory, and volume for this data to be stored. The files are stored on the server's volume you designate.

## OTM Requirements for the NDMP Host

In addition to meeting the installation requirements listed in "Installation Requirements" on page 5, the NetWare media server serving as the NDMP host must also have:

◆   OTM installed.

◆   Sufficient free space on the volume containing the cache file. This amount depends on the amount of file changes that occur during a backup; a minimum of 40 MB of free disk space is required after installation.

◆ Sufficient memory to mount a duplicate of the volumes that are being protected.

◆ 16K free space on the DOS partition for the OTMDSK.DSK driver if you are using DSK disk drivers.

◆ Volumes that are IDE or SCSI devices; I20 and SSA drives are not supported.

The volumes you want to back up with OTM must be traditional NetWare volumes; NSS volumes are not supported.

**Note** OTM cannot be used on CD-ROM drives, floppy disk drives, or the media server's DOS partitions.

The volume containing the cache file must have at least 40 MB of available space. For information about changing the location of the cache file, see

## Creating a Backup Job Using OTM

To create a backup job using OTM, the policy used for the backup must contain the environmental variable DO_SNAPSHOT=1.

▼ **To set the OTM variable:**

1. Select the policy that will be used for this backup.

2. Select the **Files** tab.

3. Above the list of files that you want backed up using OTM, type

   ```
   set DO_SNAPSHOT=1
   ```

**Note** The set command entry must occur in the file list before the directories and files to which it applies.

4. Save the policy, and then complete a backup following the procedures described in "Performing a Backup" on page 29.

## Configuring OTM Settings

It is strongly recommended that you use the default settings for OTM. However, if these default settings are not appropriate for the environment your server or volume is in, you can change the OTM configuration file settings in the NBUSRVR.CFG file in the *<SERVER NAME>*\SYS:\VERITAS\NBU directory. The settings are described in the following tables.

You may elect to change the following options:

| Setting | Option |
|---------|--------|
| **Note** All numeric values are in hexadecimal format. The value appearing in parentheses is the corresponding decimal value. | |
| Otm_CacheFileName=<vol:\path> | Name and location of the OTM buffered data file. The default is SYS:\SYSTEM\OTM01. This option could be used to move the cache file to a volume containing more disk space. |
| Otm_SizeOfCacheFileMB=n | Size of the cache file buffer that will be used for the capture of the volume for backup. The default is 28 (40) MB. This value must be smaller than the setting for Otm_MaxSizeOfCacheFileMB and should be increased if you are repeatedly seeing error messages that there is not enough disk space. The maximum is FFF (4095). |
| Otm_MaxSizeOfCacheFileMB=n | Maximum allowable size of the buffered cache file. This value must be larger than the setting for OTM_SizeOfCacheFileMB. The default is 64 (100) MB. (For this release, this option is not used.) |
| Otm_PreOpenFileName=<filename> | Name of the NCF file to execute immediately before OTM captures a volume. This NCF file may have commands instructing other applications to cease writes for a moment. The default is PREOPEN. |
| Otm_PostOpenFileName=<filename> | Name of the NCF file to execute immediately after OTM has captured a volume. This NCF file can restart the writes of applications ceased by the PREOPEN NCF file. The default is POSTOPEN. |
| Otm_PostCloseFileName=<filename> | Name of the NCF file to execute immediately after OTM has released the captured volume. The default is POSTCLSE. |

| Setting | Option |
| --- | --- |
| Otm_QuiescentWait=n | Number of seconds that a volume has to be quiet before it will be captured for backup. A volume is considered quiet if no writes occur during the waiting period. The default waiting period is 5 (5) seconds. Reducing this value increases the likelihood that a quiet period occurs, but decreases the chance that open files on the volume are captured in a usable state. Increasing this value makes it less likely that VREPAIR will run. You may make the value 0 on systems that are having trouble meeting the quiescent wait, but this may cause VREPAIR to load. |
| Otm_QuiescentTimeout=n | Number of seconds that should pass before OTM stops trying to capture a volume for backup. If the volume cannot be captured during this time, then the capture will abort and a time-out error will be issued. The default is 258 (600). |

The following options should only be changed at the direction of technical support:

| Setting | Option |
| --- | --- |
| Otm_Flags=n | For internal use only. The default is 3 (3). |
| Otm_MinimumThreadCount=n | Minimum number of threads that can be created to handle disk writes during an Open File Option backup. The default is A (10). |
| Otm_MaximumThreadCount=n | Maximum allowable threads that can be created to handle disk writes during an Open File Option backup. The default is 1E (30). |
| Otm_ThreadStartupDelay=n | Number of seconds Open File Option will delay before creating another thread to handle outstanding disk write operations. The default is 2 (2). |
| Otm_DeadlockTimeout=n | Number of seconds before a deadlock situation is diagnosed and identified. When a deadlock situation is encountered, all virtual volumes that are being backed up with OTM are terminated and released. The default is 1E (30). |
| Otm_Username=n | For internal use only. The default is <nothing>. |

| Setting | Option |
|---------|--------|
| Otm_Password=<password> | For internal use only. This field is blank by default. |

# Using the NetWare Media Server Option With a Cluster

Server clusters provide high availability and manageability of critical network resources, including data (volumes), applications, server licenses, and services. In a server cluster, two or more servers (called *nodes*) are linked in a network, and run cluster software that allows network resources to be tied to a cluster rather than to individual network servers. With cluster-enabled volumes, your data and applications appear to be provided by a single system, even though the cluster may be composed of several network servers.

When one node fails, the failed node's applications and volumes are transparently restarted on a surviving node (called *failover*) by NetBackup. During failover, most users will not even be aware of the failure.

When the node that failed returns to service, the volumes newly acquired by the failover node migrate to the controlling node (called *failback*).

In a cluster environment, the NetWare Media Server Option is installed on each node in the cluster.

All nodes must be in the same NetWare Directory Services (NDS) tree, must be configured with the IP protocol, and must be on the same IP subnet.

To fully protect your clustered servers, create backup jobs for each node in the cluster for only the volumes normally mounted to the node. To automatically protect all volumes during a failover, create another backup job for each node that protects all volumes that *could* mount on the node during failover.

The backup job containing the clustered volume will always fail except during failover (when the volume is actually mounted on the node).

When restoring in a cluster environment, restores are performed in the same way as in a non-clustered environment (see ).

# Using Intelligent Disaster Recovery 5

This section details how to use the Intelligent Disaster Recovery (IDR) Option, an option designed to help you quickly and efficiently recover your Novell NetWare 4.2x and 5.x servers after a catastrophic disaster.

*Using Intelligent Disaster Recovery* contains the following topics:

| Section | Describes |
| --- | --- |
| "About the Intelligent Disaster Recovery Option" on page 38 | Key benefits and features of the IDR option. |
| "Requirements for Using IDR" on page 39 | Requirements for installing and using IDR. |
| "Pre-Disaster Preparation" on page 40 | An overview of the IDR preparation steps and how to launch the Intelligent Disaster Recovery Wizard. |
| "Recovering from a Disaster" on page 43 | Procedures for recovering your NetWare servers after a disaster occurs. |
| "Tips for Maximizing Protection" on page 45 | Suggestions for ensuring the maximum protection for your NetWare servers. |
| "NDS Preparation and Recovery Notes" on page 49 | Information on NDS disaster preparation and recovery. |
| "Command Line Parameters" on page 51 | The command line parameters used with IDR. |
| "Using Other Media Types" on page 57 | Which media types can be used to protect your data. |
| "Frequently Asked Questions" on page 58 | Questions frequently asked about IDR, disaster planning, and disaster recovery. |

# About the Intelligent Disaster Recovery Option

IDR provides a fully automated disaster recovery solution that allows you to quickly and efficiently recover your Novell NetWare servers running the NetWare Media Server Option.

IDR supports NSS volumes, allowing you to quickly get your whole NetWare server up and running again in the event of a disaster.

IDR supports the creation of a CD bootable image file that can be used with a CD burner to create bootable CDs. This disaster recovery solution is intended to recover the NetWare server and requires only the latest full backup media to completely recover a system.

You can also generate floppy disks from the CD bootable image on a local Windows workstation, cutting down on floppy creation time.

If you do not elect to create and use CD bootable images, you can create floppy disks at the server. This disaster preparation effort requires you to down your server, format some floppy disks, install and run the software, and then insert those floppy disks when the on-screen instructions prompts for them.

## Choosing the Bootable Media

When creating bootable media through IDR, you can create:

◆ Floppy disks

◆ CD-Recordable (CD-R) or CD-Rewritable (CD-RW)

Consider your available hardware and your system BIOS when selecting the type of bootable media you create.

For example, bootable CDs require a BIOS that supports booting from a CD-ROM and third-party CD writing hardware and software to allow burning of ISO 9660 CD images.

Bootable CDs provide faster preparation and recovery than floppy disks; however, floppy disks work on most systems. You can also generate floppy disks on a local workstation from the CD bootable image file NBUDRCD.ISO, which resides in the SYS:\VERITAS\NBU\IDR directory, eliminating the need to down the server for IDR preparation.

# Requirements for Using IDR

The following requirements are necessary to protect your servers:

◆ Your system must be running NetWare versions 4.2x or 5.x with the latest service packs.

◆ One current full backup of the NetWare server made with NetBackup for NDMP must be available from which to restore.

◆ `Format.com` must be available.

**Note** If using NetWare 5.x, you may need to copy format.com from your license disk.

Additional requirements for using CD-R or CD-RW as the bootable media include:

◆ A BIOS that supports booting from a CD-ROM.

◆ Third-party CD writing hardware and software to allow burning of ISO 9660 CD images.

Additional requirements for using floppy disks as the bootable media include:

◆ Floppy disks must be available during the preparation of this protection scheme.

**Note** It is strongly recommended that you run chkdsk/scandisk on the floppy disks to verify their integrity.

◆ The DOS program `Format.com` must reside on the bootable DOS system disk.

You may also want to have:

◆ One current full backup of the NetWare server's DOS partition made with NetBackup for NDMP using the included Novell TSADOSP.NLM.

◆ A backup made of the NBUDRCD.ISO file after it is created. (You could also copy this file to a local workstation.)

◆ An alternative removable media, such as Superfloppy, Jaz, or Zip disk to speed up the preparation and recovery processes if not using bootable CD.

# Pre-Disaster Preparation

To successfully recover from a disaster, you must properly prepare for it ahead of time. No matter which bootable media you plan to use, the pre-disaster preparation steps should be performed whenever you:

◆ Add new support packs.

◆ Upgrade your system's operating system.

◆ Modify your hardware configuration.

◆ Add or modify volumes on your server.

> **Note** If the REMOVE DOS command has been executed from your system console, the Intelligent Disaster Recovery preparation will not work. Down the server and reboot; do not issue the REMOVE DOS command; if the command is found in the AUTOEXEC.NCF file, edit the file and remove the command. Down the server and reboot it.
>
> If NetWare Media Server Option is installed on your server, it must be loaded but not actively running jobs.

## Pre-Disaster Preparation for Bootable CD

If you plan to use a CD as your bootable media, you must create the CD bootable image file, and then use third-party software and hardware to place that file on a CD. Your bootable CD and your most recent backups can then allow you to restore your server to its pre-disaster state.

▼ **To run IDR preparation for bootable CD:**

**1.** At the system prompt:

```
load nbudr -b -a
```

The preparation process creates the CD bootable image file, NBUDRCD.ISO, in the SYS:\VERITAS\NBU\IDR directory.

WHICH DIRECTORY?

> **Note** You must use third party CD writing hardware and software to allow burning of this ISO file on the CD.

You should ensure your computer is capable of booting from the CD (see "Recovering Using a Bootable CD" on page 43).

# Pre-Disaster Preparation for Floppy Disks

If you plan to use floppy disks for your bootable media, run pre-disaster preparation steps at the server that include first creating a boot disk and then copying information required to protect your server on floppy disks.

You will need a number of blank, formatted disks if you want to use disks as your bootable media. This number will vary depending on the version of NetWare and other software you have installed in your server.

Number of Disks Required

| MINIMUM # OF DISKS REQUIRED FOR THE MEDIA SERVER | MINIMUM # OF DISKS REQUIRED FOR THE REMOTE NETWARE SERVER |
| --- | --- |
| NetWare 5.x - 13 disks | NetWare 5.x - 11 disks |
| NetWare 4.x - 9 disks | NetWare 4.x - 6 disks |

Label the disks as requested by the preparation process.

**Note** You can substitute alternative media such as Zip, Jaz, or hard disk space (not containing the NetWare partition) in place of floppy disks during the server-based pre-disaster preparation phase. For instructions on using these alternative media types, see "Using Other Media Types" on page 57.

If you elect to generate floppy disks as your bootable media, the first step is to create a boot disk that is used to start the recovery process.

**Note** It is critical that the boot disk be created properly, and that the server can be successfully booted to DOS when it is used.

▼ **To create the boot disk:**

1. Label the floppy disk *Disaster Recovery System disk*.

2. To format the disk as a system disk, down the server and format the disk using the following command:

   ```
   Format A: /s
   ```

3. Copy the DOS programs FORMAT.COM and FDISK.EXE to the disk.

**Note** The safest way to create the Disaster Recovery System disk is to follow these steps. By creating the disk at the server, you are ensuring that the correct version of DOS is placed on the disk, and that the appropriate versions of FORMAT.COM and FDISK.EXE are used. Additionally, not all disk drives are identical although it is more likely that disks created in the drive can be read by that drive; however, we understand that there are servers that you cannot afford to arbitrarily bring down. If this is the case, you can create the Disaster Recovery System disk at another workstation as long as you are using the same versions of DOS, FORMAT.COM, and FDISK.EXE that are on the server you want to protect. *Do not* use Windows 95/98 DOS.

Now that you have a system disk, along with blank disks, it is time to collect the information required to protect your server.

**Note** If the REMOVE DOS command has been executed from your system console, the Intelligent Disaster Recovery preparation will not work. Down the server and reboot; do not issue the REMOVE DOS command; if the command is found in the AUTOEXEC.NCF file, edit the file and remove the command. Down the server and reboot it.

**Note** NetWare Media Server Option must be running on the server in order to allow the preparation utility to detect the appropriate NetWare Media Server Option files necessary to recover the server data. If you have not installed NetWare Media Server Option, install it and do a full backup of your server before continuing.

▼ **To continue server-based IDR preparation using floppy disks:**

1. Start Intelligent Disaster Recovery for NetWare by typing, at the system console prompt:

   ```
   load nbudr -b
   ```

2. Insert each disk as prompted.

3. After all disks are created, the verification process begins automatically. It is important that you verify the disks.

**Note** If you cannot verify the disks at this time, you should run the command LOAD NBUDR -C as soon as possible. This option allows you to verify the contents of the IDR preparation disks.

In the event of a disaster, the disaster recovery disks and your most current backup media (Full and Differential or Incrementals) are the only items required to perform a complete and automated recovery of your server. For more information about restoring your server using your disaster recovery disks, see "Recovering Using Floppy Disks" on page 43.

# Recovering from a Disaster

If your server were to crash right now, you would need the following in order to recover it with Intelligent Disaster Recovery for NetWare:

◆ The backup of basic DOS, NetWare, and NDS information generated by Intelligent Disaster Recovery for NetWare.

◆ A full backup of the server's data.

◆ Any DOS device drivers required to access the media containing the Intelligent Disaster Recovery information, such as Zip device drivers, SCSI drivers, etc. (see "Using Other Media Types" on page 57).

## Recovering Using a Bootable CD

Disaster Recover using a bootable CD requires only the bootable CD and the most recent backups.

▼ **To boot a computer using a bootable CD:**

**1.** At the computer being recovered, ensure the bootable CD created by IDR for NetWare is inserted into the CD-ROM.

**2.** Follow on-screen instructions.

**Note** If you are testing your bootable media, do not continue when prompted that the Disaster Recovery process will begin. Instead, remove the CD, press <F3>, and reboot the server.

## Recovering Using Floppy Disks

If you experience a catastrophic disaster, restore the hardware to a working state and then boot your server using the *Disaster Recovery System Disk*. After the system initializes, follow the on-screen directions. Intelligent Disaster Recovery for NetWare automatically rebuilds both partitions and volumes, and installs a copy of NetWare Media Server Option, which enables you to restore all data from your media.

After reaching this point, restore all of this server's files using NetBackup. For more information, refer to your NetBackup Administrator's Guide.

**Note** It is important to understand that Intelligent Disaster Recovery for NetWare leaves your NetWare server in a minimal system state. This means that only the files necessary for NetWare to run have been restored. Everything else must be restored from the media containing the Full backup job, or reinstalled manually.

## Recovery Notes

◆ During a recovery, your system must have the same number of hard drives installed as it did during the disaster recovery preparation phase. If you are restoring to a server with a different hard drive configuration, see "Frequently Asked Questions" on page 58.

◆ If Intelligent Disaster Recovery for NetWare cannot repartition the DOS partition, you can manually repartition and format it using the FDISK.EXE and FORMAT.COM programs found on the Disaster Recovery System disk.

After rebuilding the DOS partition, run NBUDRAPP -F at the DOS prompt from the Disaster Recovery System disk.

**Note** The -F parameter begins the recovery operation at the point where the DOS files are restored.

◆ If, after a catastrophic disaster, you rebuild your server with a larger hard drive or drives, Intelligent Disaster Recovery will, during the recovery process, recognize the extra space and prompt you to allocate the extra space to the original non-mirrored NetWare partition. Answer **Yes** to the prompt to increase the NetWare partition size by the amount of extra disk space found by the Intelligent Disaster Recovery procedure.

◆ If you use a Boot Manager (System Commander, NT, OS/2, etc.), only the current (DOS) configuration will be recovered.

◆ If you replace a protected drive with one that already contains a DOS partition and the new drive's DOS partition is not the same size as the original, Intelligent Disaster Recovery will want to repartition the new drive to match the original drive's partition size. If you do not want this done, then use FDISK along with FORMAT to manually create the DOS partition size you want.

After manually creating the DOS partition, start NBUDRAPP using the -F parameter to restore the DOS Disaster Recovery Files disk(s).

> **Note** When manually repartitioning the DOS partition on the new hard drive, make sure there is enough unpartitioned space left on the drive for the NetWare partition.

◆ If you are using an IBM computer and the drive containing the system's configuration information fails, you must reconfigure the system using the IBM Reference disk prior to running recovery.

◆ If you are using a Compaq computer and the drive containing the System Configuration Partition fails, Intelligent Disaster Recovery will re-create the partition on the new hard drive; however, you must use the Compaq SmartStart utilities to update the system partition.

# Tips for Maximizing Protection

This section offers you tips on gaining additional protection for your NetWare server data by allowing you to modify specific components of Intelligent Disaster Recovery for NetWare. These tips include:

◆ Modifying certain .INI files to include additional files for protection

◆ Protecting your server's *entire* DOS partition using Novell's TSADOSP.NLM

It also offers details about Intelligent Disaster Recovery for NetWare's LOG file and the role it plays in the disaster recovery process.

> **Note** To maintain peak server efficiency and to ensure a complete update to the NDS Recovery disk, enter a value of five minutes in the **Delay after command (seconds)** field on the policy's Pre/Post Options dialog box (for example, 300).

After the backup job runs, Intelligent Disaster Recovery for NetWare starts and the NDS Recovery Files disk 1 update begins.

## Modifying the .INI Files

Intelligent Disaster Recovery for NetWare uses three .INI files to create a set of recovery disks for your server. These files, installed in the server's SYS:\VERITAS\NBU directory, include:

◆ *SYSFILES.INI.* Used to create the Disaster Recovery System disk.

◆ *DOSFILES.INI.* Used to create the DOS Recovery Files disks. It specifies the recovery-critical files to be backed up from the server's *DOS partition*.

◆ *NETFILES.INI.* Used to create the NetWare Disaster Recovery Files disks. It specifies the recovery-critical files to be backed up from your server's *SYS: volume*.

Each file is a template used by Intelligent Disaster Recovery for NetWare to back up the default file configurations needed to get your server up and running in a minimal state.

You can edit these files to add files and directories you want to protect; however, the SYSFILES.INI and the NETFILES.INI are designed to cover a wide range of environments so it is not necessary to customize them for your server.

If you want to add other files to the protection process, edit the .INI files and add their path and filename designations.

For example, to add all files residing in the C:\SCSI directory on your DOS partition to DOSFILES.INI, edit the file and add the directory location to the existing path and filename designations.

```
Example Editing the DOSFILES.INI presents you with the
        following structure. Add the desired path at the end
        of the DOS file area.

[DOS]
FILE=C:\AUTOEXEC.BAT
FILE=C:\CONFIG.SYS
FILE=C:\DOS\EDIT*.*
FILE=C:\DOS\FORMAT.*
FILE=C:\DOS\HIMEM.SYS
FILE=C:\DOS\QBASIC.EXE
FILE=C:\DOS\SYS.*
FILE=C:\SCSI\*.*

[NETWARE]
FILE=%BOOT_DIR%\ETHERTSM.NLM
FILE=%BOOT_DIR%\FDDITSM.NLM
FILE=%BOOT_DIR%\ICMD.NLM
etc...
```

Make sure that as you add filenames, you spell them correctly. Intelligent Disaster Recovery for NetWare will not notify you of an error if it cannot find the specified file.

Certain files, by default, are not backed up, although they are listed in the .INI files.

For example, the PATCH directories for NetWare versions prior to 4.2 are not backed up in the DOSFILES.INI file by default because adding them increases the number of disks required during the disaster recovery preparation phase. However, you may decide that these files are important and must also be protected.

To include them, edit the file and add the following:

```
Example

FILE=%BOOT_DIR%\PATCHES\NATIVE\*.*
```

> **Note** If you did not install the patches to the %BOOT_DIR%\PATCHES\NATIVE
> directory, you must change the FILE= line to reflect where the patches were
> installed.
>
> There are placeholders in DOSFILES.INI designated as %BOOT_DIR%. These
> placeholders are replaced by the actual boot directory when Intelligent Disaster
> Recovery for NetWare runs.
>
> *Do not edit these placeholders.*

> **Note** During installation, Intelligent Disaster Recovery for NetWare places the .INI files in
> the SYS:VERITAS\NBU directory. Review the .INI files to ensure the correct path
> locations for the specified files. For example, C:\DOS is the path DOSFILES.INI
> looks for when backing up DOS files on your system; however, if you installed DOS
> files elsewhere, the path location needs to be updated to reflect this.

## Using TSADOSP.NLM

Included with Intelligent Disaster Recovery for NetWare is a Novell-supplied TSA named
TSADOSP.NLM. Using this TSA allows you to completely backup and restore your
server's DOS partition.

After loading this TSA, perform a full backup of your server, including the complete DOS
partition. To include the DOS partition in your backup job, select the DOS Server Partition
TSA agent, which appears in the backup sources list under the name
SERVER_NAME.DOS Server Partition TSA.

> **Note** This TSA switches the processor into *real mode* to access the DOS partition data. This
> causes a degradation in server performance during the backup operation. Backups
> of the DOS partition should be reserved for times when the server is not being
> heavily used.

Because NetBackup must run in *synchronous mode* when using TSADOSP, the Intelligent
Disaster Recovery installation program automatically adds the -s (synchronous mode)
switch to the NBUSTART.NCF file for you.

This switch should only be removed if you *do not* plan on performing operations with
TSADOSP or plan to use post commands to run the disaster recovery preparation of NDS.

# The Intelligent Disaster Recovery Log File

The Intelligent Disaster Recovery Log file is found in the SYS:VERITAS\NBU directory. The file, named NBUDR.LOG is an ASCII text file that is created during the initial Intelligent Disaster Recovery for NetWare preparation process. Information is appended to the file as subsequent disaster recovery updates are completed.

**Note** During the recovery of a server, a NBUDR.LOG file is created in the server boot directory on the DOS partition. This file can be viewed to review the disaster recovery process after the NetWare server has been recovered. The NBUDR.LOG file is also copied to the system control disk and *should* be reviewed to ensure everything you will need during a recovery was gathered.

The log file contains four sections, each detailing information contained on the set of disaster recovery disks created earlier. Refer to the following example:

```
Example

#
MON Mar 10 12:29:28 1997
#


-----------------------------------------------------
SYS:VERITAS\NBU\SYSFILES.INI
-----------------------------------------------------

SYS:VERITAS\NBU\NBUDIAG.FAX
SYS:VERITAS\NBU\NBUDRAPP.EXE
SYS:VERITAS\NBU\NBUDREPP.RES
SYS:VERITAS\NBU\NLMS\NBUDR.NLM
etc...


-----------------------------------------------------
SYS:VERITAS\NBU\DOSFILES.INI
-----------------------------------------------------

C:\AUTOEXEC.BAT
C:\CONFIG.SYS
C:\DOS\HIMEM.SYS
C:\DOS\QBASIC.EXE
C:\NWSERVER\ETHERTSM.NLM
etc...


-----------------------------------------------------
SYS:VERITAS\NBU\NETFILES.INI
-----------------------------------------------------

SYS:SYSTEM\NBUSTART.NCF
```

SYS:SYSTEM\NBUSTOP.NCF
SYS:VERITAS\NBU\NBU.BIN
SYS:VERITAS\NBU\ADSMCFG.BIN
etc...

-----------------------------------------------------------
[Server Specific Data --> Single-Server Tree
-----------------------------------------------------------

# NDS Preparation and Recovery Notes

One of two NDS Tree Types that may reside on your server determines the preparation contents of the NDS Recovery Files disk(s). The two tree types are:

◆  Multiple-Server Tree (Replication present)

◆  Single-Server Tree (No replication present)

## Multiple-Server Tree (Replication present)

In this environment, only the Server Specific Information contained in the file SERVDATA.NDS is updated, compressed and copied to the NDS Recovery Files disk. The data contained in this file allows for the recreation of the Directory Services Database in the event the hard disk(s) containing the SYS volume fails. Because this is an automatic process, the only intervention on your part will be to log in to the directory. Because the Multiple-Server Tree environment uses replication to update NDS, it is important to understand that once you restore the Server Specific Information from the NDS Recovery Files disk, you should *not* restore Directory Services from media.

> **Note**  If your server held a master replica of any partition, use DSREPAIR to designate a new master replica on a different server in the replica ring. Intelligent Disaster Recovery for NetWare prompts you to perform this at the appropriate time during the recovery process (you can also perform this operation prior to performing the recovery). A list of servers in the replica ring is contained in the NBUDIAG.FAX file on the *Disaster Recovery System* disk.

## Changing the Replica Type

To change the replica type, run DSREPAIR on another server in the replica ring that has an active read/write replica of the partition. Use the following steps:

**1.** Load DSREPAIR.

The **Available Options** menu is displayed.

**2.** Select the **Advanced Options** menu.

**3.** Select **Replica and Partition Operations**.

**4.** Choose the partition to edit.

**5.** Select **Designate this server as the new master replica**.

**6.** Then, to make sure that time synchronization is set properly, enter the following commands on the server designated to contain the master replica:

```
set default time server type = single
set timesync type = single
set timesync restart flag = on
```

**Note**  If you intend to leave the master replica on this server, enter the following line in the AUTOEXEC.NCF file:

```
set default time server type = single
```

## Single-Server Tree (No replication present)

In this environment, the entire Directory Services database is compressed and copied to the NDS Recovery Files disk. Because the entire database is placed on the disk, it is extremely important to keep the information on the disk(s) up-to-date. For example, whenever you add or remove replicas, partitions, volumes, users, and printers.

After this information is restored and the database is opened, NetWare Directory Services is returned to the state it was in at the time of the last NDS Recovery Files disk preparation. You should only have to restore from media those individual objects that had been added since the last preparation. Likewise, you may also have to delete any objects (using the NWAdmin or NetAdmin programs) that were deleted since the last preparation.

# Command Line Parameters

The following tables explain the command line parameters that can be used with Intelligent Disaster Recovery for NetWare.

Some switches may be combined. For example, to do a restore of NDS only, while using a zip drive for the IDR media, you would need to use either the **-E** or the **-I** and **-T<drive>** switches with the LOAD NBUDR command.

NBUDR.NLM Server Preparation/Recovery Application Commands

| Switch | Operation | Description |
|---|---|---|
| -A | Perform disaster recovery image file creation or recover from a bootable CD. | This option creates the bootable image file NBUDRCD.ISO in the SYS:\VERITAS\NBU\IDR directory or performs disaster recovery from a bootable CD. |
| -A<volume> | Redirect the ISO and data files to another volume. | This option redirects the ISO and data files to another volume. This option may be used if there are free space issues with the SYS volume.<br><br>**Note** There must be at least 55 MB free space on the SYS volume for the ISO image to be copied from the alternate volume back to the SYS:\VERITAS\NBU\IDR directory. If the ISO file does not reside on the SYS directory, it will not be copied to tapes. |
| - B | Perform disaster recovery preparation | This performs a Full disaster recovery preparation. For example, load nbudr -b. |
| - C | Perform a verification of prepared disks | This option allows you to verify the contents of the Intelligent Disaster Recovery preparation disks whenever you desire. |
| - D | Perform DOS Partition disaster recovery preparation only | This backs up only the files listed in the DOSFILES.INI file. |

NBUDR.NLM Server Preparation/Recovery Application Commands (continued)

| Switch | Operation | Description |
|---|---|---|
| - E | Perform EMERGENCY NDS Disaster Recovery | Used only with NetWare version 4.1x or greater, this is used only as a last resort if NDS becomes corrupt and used only for single server trees.<br><br>Using the command `LOAD NBUDR -E`, allows you to manually restore your NDS information from the NDS Disaster Recovery disk. |
| - F | Restore DOS and NetWare recovery files | This restores DOS and NetWare recovery files. |
| - I | Force use of Only Server in NDS Tree | Used only with NetWare 4.2 or greater, this is used only when the software incorrectly determines that the server is in a multi-server tree. This is denoted during NDS file preparation as<br>[Server Specific Data --> Multi-Server Tree]. |
| - L <language> | Language-specific parameter where <Language> = (E)nglish, (F)rançais, (D)eutsch and E(s)pañol | This is used to select the English, French, German, and Spanish languages. |
| - M | Use monochrome display | This forces the system to use monochrome instead of color. |
| - N | Perform NDS disaster recovery preparation only | Used only with NetWare 4.2 or greater, this backs up only the server-specific information required to recover NDS. |

NBUDR.NLM Server Preparation/Recovery Application Commands (continued)

| Switch | Operation | Description |
|---|---|---|
| -P<path> | Specify path where FORMAT.COM file resides. | Used during the creation of the bootable image file to specify the path where your FORMAT.COM file resides. If NBU????? finds more than one FORMAT.COM on your system, you will be prompted to choose the correct one to use. This option allows you to specify which FORMAT.COM file to use without being prompted. If you do not have a copy of FORMAT.COM for your server on the boot disk, which would occur if you installed from a Novell bootable CD, you can specify a path on a floppy disk (`LOAD NBUDR -B -A -PA:\`).<br><br>**Note** Novell's NetWare 5 license disk contains a copy of FORMAT.COM. |
| - R | Perform Disaster Recovery | This performs the actual recovery of a server, and this parameter is normally issued only from the application.<br><br>**Note** If you lose a drive that does not contain any portion of the SYS: volume, you can use the -R option to recover just the affected partitions and volumes: Enter **No** when prompted to delete existing partition(s). Next, abort the operation when the first recovery files disk is requested. Next, if running NetWare 4.2, restore the volume information by first restoring the volume object from an NDS backup. Then restore the data. |

NBUDR.NLM Server Preparation/Recovery Application Commands (continued)

| Switch | Operation | Description |
|---|---|---|
| - S | Update Storage Environment only | This updates the information on the Disaster Recovery System disk after you add additional drives and volumes to the system. |
| - T<drive> | Allows you to use any DOS-recognized device to recover your Intelligent Disaster Recovery data files (see "Using Other Media Types" on page 57). | Using the − T<drive> parameter specifies where all data files normally written to the disaster recovery support disks (DOS Recovery disks, NetWare Recovery Files disks, and the NDS Recovery Files disks) are to be recovered from. |
| - U | Update Disaster Recovery System disk only | This includes the storage information (partitions and volumes), and the files listed in the SYSFILES.INI file. |
| - V | A viewing parameter | This enables the viewing of the storage information contained in the Control File (NBUDR.BIN), located on the Disaster Recovery System Disk. |
| - Z | For use with *bootable* Zip drives and other similar *bootable* devices | − Z tells Intelligent Disaster Recovery that Drive A: is a bootable Zip drive or other similar device. |

NBUDRAPP.EXE Command Line Parameters

| Switch | Operation | Description |
|---|---|---|
| -A | Start disaster recovery process from a bootable CD. | This option starts the disaster recovery process using a bootable CD. |
| - F | Restore DOS and NetWare recovery files | This restores DOS and NetWare recovery files. |
| - M | Use monochrome display | This forces the system to use monochrome instead of color. |

NBUDRAPP.EXE Command Line Parameters (continued)

| Switch | Operation | Description |
|--------|-----------|-------------|
| - T\<drive\> | Allows you to use any DOS-recognized device to recover your Intelligent Disaster Recovery data files (see "Using Other Media Types" on page 57). | Using the – T\<drive\> parameter uses all data files normally written to the disaster recovery support disks (DOS Recovery disks, NetWare Recovery Files disks, and the NDS Recovery Files disks) on the DOS-recognized drive specified as part of the parameter. |
| - Z | For use with *bootable* Zip drives and other similar *bootable* devices | – Z tells Intelligent Disaster Recovery that Drive A: is a bootable Zip drive or other similar device. |

The following table explains the commands that can be used with the disk creation utility, MKIDRDSK.EXE.

MKIDRDSK Command Switches

| Switch | Operation | Description |
|--------|-----------|-------------|
| /D | Generate only the DOS images , or when used in with the /F command, generate only the DOS images and disks. | This command creates images of the DOS floppy disks needed for disaster recovery from the image file, and places these images on the media server. |
| /F | Generate floppy disks. | This command creates and verifies all floppy disk images from the bootable image required to run disaster recovery. |
| /FO | Create floppy disks from the existing floppy disk images. | This command creates floppy disks from the current floppy disk images without generating the floppy images again. |
| /H | Display this help screen. | This command displays the help file. |

MKIDRDSK Command Switches (continued)

| Switch | Operation | Description |
| --- | --- | --- |
| /L <language> | Language-specific parameter where <Language> = (E)nglish, (F)rançais, (D)eutsch and E(s)pañol | This is used to select the English, French, German, and Spanish languages. |
| /N | Generate only images of NetWare floppy disks. If used with the /F command, generate images and floppy disks of the NetWare floppy disks only. | This command creates images of the NetWare floppy disks needed for disaster recovery from the image file, and places these images on the media server. |
| /S | Generate only an image of the *Disaster Recovery System* disk. If used with the /F command, generate image and floppy disk of the *Disaster Recovery System* disk only. | This command creates an image of the Disaster Recovery System disk from the image file, and places this image on the media server. |
| /T | Generate only images of NDS floppy disks. If used with the /F command, generate images and floppy disks of the NDS floppy disks only. | This command creates an image of the NDS floppy disks, and places this image on the media server. |
| / V | Verify disk images. | This command verifies the disk images. |
| /Z | Turn on debug. | This command places the MKIDRDSK utility in debug mode. |
| /ZL | Turn on debug with logging. | This command places the MKIDRDSK utility in debug mode and create a log file. |

# Using Other Media Types

This section discusses the most common Disaster Recovery preparation procedures using media other than disks. Instead of using disks to create the Intelligent Disaster Recovery disks, you can use the following media types if you have them installed on your system:

◆ Iomega Zip drives

◆ Iomega Jaz drives

◆ Hard disk drives that contain a DOS partition but do not contain a NetWare partition

Using these devices speeds up Intelligent Disaster Recovery for NetWare's disaster recovery preparation and collection process.

## Using Zip, Jaz, or Hard Disk Space

Rather than using a set of floppy disks during pre-disaster preparation and server information collection phase, you can use Zip or Jaz cartridges, or hard disk space; however these devices must be seen under DOS, and be assigned a DOS drive letter.

You will still need to create a Disaster Recovery System disk. After creating this system disk, make sure ALL drivers required for the Zip, Jaz, or hard disk drives are copied to the system disk.

1. Create a bootable Disaster Recovery System disk by downing the server and formatting a floppy disk with the following command:

   ```
   FORMAT A: /S
   ```

2. Copy FORMAT.COM and FDISK.EXE to the system disk.

3. Copy all required Zip, Jaz or hard disk drivers to the bootable system disk.

4. Reboot the server with the Disaster Recovery System disk, making sure all devices appear under DOS when the boot procedure finishes.

5. Down the server and reboot it to NetWare.

6. At the System Console, type:

   ```
   load NBUDR -B -T<Alternative media drive letter>
   ```

   For example,

   ```
   load NBUDR -B -TE
   ```

   where E is the drive letter assigned to a Zip drive under DOS.

Intelligent Disaster Recovery now collects all pertinent server recovery data and places it on the alternative media specified with the **-T** switch, instead of on floppy disks.

# Frequently Asked Questions

**I used to have three 1GB hard drives on my server when it crashed. I've replaced them with a single 3GB hard drive. How do I use Intelligent Disaster Recovery to restore my system?**

You will need to boot from the *Disaster Recovery System disk* and once loaded, press <F3> to exit to DOS. Run FDISK.EXE from the floppy and recreate the DOS Partition(s) manually.

**Note** If you don't remember the size of the DOS Partition(s) you can run NBUDRAPP -Z to display the partition information.

After the system reboots and NBUDRAPP is reloaded, press <F3> to exit to DOS. Run FORMAT.COM from the floppy to format the DOS Partition(s).

Next run NBUDRAPP -F to recover the DOS Data Files from the DOS Recovery Files disk(s) and allow the recovery process to continue to bring up NetWare. After the server is restarted and NBUDR.NLM is loaded, you are informed that *There are too few Hard Disks! Original = #, Current = #.* Press a key to exit the application. From the system console, load INSTALL and manually recreate the NetWare Partition(s) and Volume(s)

**Note** Don't forget to add the Name Spaces back to the Volume(s). If you don't remember the size of the NetWare Partition(s) or Volume(s), load NBUDR -V to display the partition information and volume information.

Next, load NBUDR -F to recover the NetWare Data Files. If running NetWare 4.2 or greater, load NBUDR -E to recover Directory Services. Once this is complete you can execute NBUSTART.NCF to start the NetWare Media Server Option. After it loads, catalog and restore the media required to get back your data.

**I used to have an IDE hard drive in my server and now I am upgrading to a SCSI drive that is a bit bigger. How do I use Intelligent Disaster Recovery to restore my server?**

Make sure the BIOS is enabled for the SCSI card (so DOS will recognize the drive without the need for additional drivers) and just perform a normal recovery. During the NetWare Partition recovery process, a prompt states that additional space is available for NetWare and gives you the option of using it.

**Note** If you don't use it you will NOT be able to allocate it to NetWare later.

The recovery process proceeds normally from this point.

**The hard disk controller in my system has changed. How do I use Intelligent Disaster Recovery to restore my system?**

Before performing the Intelligent Disaster Recover Preparation, add the additional SCSI drivers (for the new controller) to the DOSFILES.INI file in the [NetWare] section.

If you haven't done this and are using floppy disks for the recovery, reboot from the system floppy disk, and then press <F3> to exit to DOS.

Next, copy the required drivers to the server boot directory (nwserver) and edit the STARTUP.NCF file and add the new drivers.

Manually copy the AUTOEXEC.NCF from the floppy to the server boot directory and execute SERVER.EXE.

Recovery should continue normally from this point.

**The server I am restoring is not the media server. How do I use Intelligent Disaster Recovery to restore my system?**

There is no difference between installing Intelligent Disaster Recovery remotely on a remote server or locally on a media server. Make sure, however, you have a full backup of the remote server on the media server's tape drive. After the remote server backup is done, perform the Intelligent Disaster Recovery installation and preparation process on the actual remote server.

If a disaster does occur, simply perform Intelligent Disaster Recovery for NetWare's recovery process on the remote server. After the disaster recovery process completes, restore the server's data from your backup tapes.

**Why do I need to have NetWare Media Server Option loaded in order to prepare the disaster recovery floppy disks?**

This only occurs when you are doing a Disaster Recovery Preparation on a server that has NetWare Media Server Option installed. The Disaster Recovery process restores a minimal NetWare Media Server Option installation as well as getting your NetWare system to a running state. The preparation process needs NetWare Media Server Option loaded in order to determine which NLMs should be saved on the Disaster Recovery disks.

**Just the drive that has the SYS: volume failed on my server. How do I use Intelligent Disaster Recovery to restore my system?**

Run the Intelligent Disaster Recovery normally. When prompted to delete existing partitions (this happens once NBUDR.NLM is loaded and determines NetWare partitions already exist) say "No." Recovery will proceed normally.

**The tape drive that I am using to restore my system is not the same as the one that was being used when the Disaster Recovery Preparation was done for the media server. How do I restore my system?**

If the tape drive requires a media type different than what was used to do the original backup of the server, you will not be able to perform a restore.

However, if the same media can be used but the tape drives are housed in a different manner (stand-alone versus autoloader), then the NetWare Media Server Option must be re-installed before restoring the data. If you do not re-install the software, the recovery will still work, but you will get an error stating that no tape drives are found when the NetWare Media Server Option is launched.

For example, if you've replaced a stand-alone 4mm DAT tape drive with a 4mm autoloader device, you will need to re-install the NetWare Media Server Option on your server before restoring the data.

# Index